Department of Homeland Security Daily Open Source Infrastructure Report for 17 October 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports high−tech crooks are hijacking online brokerage accounts by using spyware and operating from remote locations, sometimes in Eastern Europe; this is a growing problem according to the U.S. Securities and Exchange Commission. (See item 12)
- The U.S. Customs and Border Protection has announced that it has completed installations of the Automated Commercial Environment to enhance border security at all land border ports in New York. (See item 16)
- The U.S. Food and Drug Administration reports a warning system meant to alert food companies in the event of a food poisoning outbreak failed one−third of the time in a recent government test. (See item 22)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *October 16, Los Angeles Times* — **Post−9/11 security standards not being met at uranium facility.** The Department of Energy (DOE) cannot meet its own post−September 11 security standards to repel a terrorist force at the Fort Knox of uranium, a facility in Tennessee that stores bomb−grade material, agency officials acknowledged. The material is stored in five

masonry and wood−frame buildings at the Y−12 facility, a key part of the nation's nuclear weapons infrastructure near Knoxville, TN. The National Nuclear Security Administration is building a secure facility, due to be completed in 2009, to warehouse the material. Until then, DOE has given itself an "extension," or waiver, on meeting security requirements at the site. The risk is that terrorists will gain access to highly enriched uranium and then within minutes construct a crude but powerful improvised nuclear device, or IND. It is believed such a device could have a yield equal to that of the Hiroshima atomic bomb. The issues at Y−12 were disclosed in a report by the Project on Government Oversight. At the Tennessee site, the department has 527 guards. To meet the federal security standard would have required a force of 800 guards, said Peter Stockton, one of the report authors.
Source: http://www.latimes.com/news/printedition/asection/la−na−nuke 16oct16,1,482058.story?ctrack=1&cset=true

2. *October 16, Associated Press* — **Progress being made in recovery from unprecedented snowstorm.** A fall snowstorm dumped more than two feet of snow last week in western New York, leaving three people dead and nearly 400,000 homes and businesses without power. Hospitals, senior centers, water and sewage treatment plants and other key operations were being given priority as National Grid and New York State Electric & Gas (NYSEG) crews continued round−the−clock efforts to restore power. Nevertheless, it could take up to a week to restore power to some individual homes in outlying areas, utility officials said. NYSEG reported it still had 74,000 customers without power Sunday evening, October 15. National Grid said it had about 180,000 residential and commercial customers without power. Some 392,000 homes and businesses were left powerless in the storm's immediate aftermath, including about 70 percent of the city of Buffalo. Crews from New York, Pennsylvania, Massachusetts, and Rhode Island were sent to help western New York get back up to full power.
Source: http://www.auburnpub.com/articles/2006/10/16/news/state/stat e02.txt

3. *October 15, Associated Press* — **Government probers say refinery short on safety.** BP did not have safety procedures in place which could have prevented a July 2005 fire that broke out at its Texas City refinery because workers installed the wrong type of pipe, federal investigators said Sunday, October 15. The fire caused more than $30 million in damage. A report by the U.S. Chemical Safety and Hazard Investigation Board said maintenance workers had replaced three pipe segments, substituting one of them with a type of steel that couldn't resist the effects of high−temperature hydrogen. That segment failed after less than 3,000 hours of operation. Procedures at the refinery did not require testing of critical piping during maintenance to ensure that the right material was used, it said. The report also said BP had not warned the maintenance contractor that the two types of steel were not interchangeable. BP has created a testing program like one federal investigators called for, spokesperson Neil Chapman said.
Source: http://news.yahoo.com/s/ap/20061015/ap_on_re_us/plant_explos ion_1

4. *October 13, Walla Walla Union−Bulletin (WA)* — **Thieves steal gear from Hat Rock Substation.** The Bonneville Power Administration (BPA) is offering up to $25,000 for information leading to the conviction of the persons who recently burglarized BPA's Hat Rock Substation, about eight miles east of McNary Dam in Umatilla County, Washington. On Friday, October 6, a BPA employee discovered thieves had cut and stolen copper grounding wire from equipment inside the energized substation yard, according to BPA. The Umatilla County

Sheriff's Office responded and is investigating the incident. In the Hat Rock incident, the damage the thieves caused did not result in a power failure and no one was injured. BPA has seen a significant increase in metal theft from its facilities over the past several months due in large part to the high price of metals on the salvage market. There have been more than 40 burglaries at BPA substations this year. A conservative estimate of damages for these crimes is $130,000, but the actual amount is likely much higher as this figure doesn't include labor−related costs associated with repairing the damage.
Source: http://www.union−bulletin.com/articles/2006/10/13/local_news /local04.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *October 13, Federal Computer Week* — **Boutelle: Army too dependent on commercial satellites.** One of the greatest technological challenges in Iraq has been the lack of bandwidth needed to push increasing levels of information to soldiers and commanders on the battlefield. Recently, the use of commercial satellites and other technologies has provided that bandwidth, but at a high cost. The Army now uses commercial sources for 80 percent of its satellite−based network bandwidth in Iraq. It costs the Army more than $1 billion last year, with one−third going to satellite leases and two−thirds to services, according to Army officials. The Army can deliver classified, unclassified and secret data anywhere in the world by bringing in satellite terminal links and transponders. But using commercial satellites is expensive, and it fails to deliver needed capabilities, said Lt. Gen. Steven Boutelle, the Army's chief information officer. "We rely so heavily on our commercial constellations today, and we need to get to a ruggedized [military] constellation," he said. The Army's goal is to give satellite capabilities to individual warfighters, he said. But commercial satellites were not designed for military use and can't do the job, he added.
Source: http://www.fcw.com/article96472−10−13−06−Web

6. *October 13, Washington Technology* — **DoD aims to improve how it buys services.** The Department of Defense (DoD) is making another attempt to improve how it buys services. Over the next three to five months, DoD will identify what services the military branches buy and put them into portfolios. Once the services are in portfolios, Defense officials will determine what the best practices are to buy them, said Shay Assad, director of Defense Procurement and Acquisition Policy. Improving the way it buys services has been an ongoing challenge for DoD. Assad added that the services would be in the portfolios by December and then over the next 12 to 18 months, DoD would come to a consensus on how to implement the best practices to buy these services. With the amount on services continuing to rise, Assad said DoD needs to focus on the need to get information systems to the warfighter and manage their procurement processes more efficiently.
Source: http://www.washingtontechnology.com/news/1_1/defense/29518−1 .html

[Return to top]

Banking and Finance Sector

7. *October 16, Register (UK)* — **Shipping sites launched by 419 scammers.** Nigerian 419 advance fee scammers operating from Amsterdam and Rotterdam have created copies of the Websites of express transportation company DHL and Lufthansa Cargo. The idea is to lure victims into paying transportation and advance fees for used motorbikes and cars that are never delivered. Now that many people are familiar with the old style 419 scam −− where an e−mail claims to come from a person needing to transfer large sums of money out of the country −− the scammers seem to have discovered a whole new way of making a quick buck. Just offer a used Suzuki Katana GSX−600 4500 or a BMZ Z3 Roadster at sites such as Car.com or Autotrader.com for next to nothing and buyers will respond. But often these cars are presently in Spain or another European country, the owner claims, so could the buyer please pay transportation costs? They then recommend the use of escrow services with slick Websites that appear legit. Some fake escrows even warn you about Internet fraud, or link to the Internet Fraud Complaint Center. The goods are never delivered.
   Source: http://www.channelregister.co.uk/2006/10/16/fake_scrows_on_t he_rise/

8. *October 16, Bank Safe Online* — **Money mules: The hidden side of phishing.** The dramatic rise in phishing and identity theft attacks includes a well−organized offline component −− the not−so−innocent "money mule" recruited by scammers to launder stolen money across the globe. The ads appear innocently on all the major employment listing sites, offering stay−at−home positions titled "shipping manager," "private financial receiver" or "sales representative." These, however, are active attempts at enlisting people −− mostly in the U.S., UK, and Australia −− to transfer illegal funds from credit card thieves operating out of the former Soviet Union, according to an investigation by iDefense. "This is the other side of phishing that most people never see or hear about. But, it's probably the most important part of the attack," said Ken Dunham of iDefense. Using hijacked PCs in well−stocked botnets, crime rings have hit pay dirt via adware installations, spam runs and phishing e−mails that attempt to trick users into entering log−in credentials on fake sites. Once the phish is successful and the malicious attacker has access to credit card and bank log−in details, there is a desperate need for a money mule in the same country as the victim to handle money transfers or to reship items to the scammer.
   Source: http://www.eweek.com/article2/0,1895,2029953,00.asp

9. *October 15, Chicago Tribune* — **Weapons of identity destruction.** Dr. Stephen Haag spends upwards of 80 hours each week on his computer, mapping out terrorist attacks. Haag, an expert in emerging technologies, believes the next attack on the U.S. will come not in the form of bombings or military movements, but from terrorists armed with computer keyboards, credit cards, and Social Security numbers. A calculated cyber identity strike could erase or manipulate the identities of millions of Americans, effectively closing the financial markets and crippling the economy. ATMs would fail, airports would shut down, banks would close −− all transactions would cease, says Haag, of the University of Denver. Haag differentiates between identity theft and identity terrorism. He says identity theft is someone stealing an identity and charging $1,500 worth of stuff. "Identity terrorism is...identity theft on steroids," he says.

Identity terrorism could strike by identity thieves selling stolen identities to a terrorist group, who would then "build weapons of identity destruction, very small pieces of software that would go out [over the Internet] for the millions of people for whom they have identities, and alter their identities within organizations, within the Social Security Administration, within First Data, within MasterCard, within airlines, ... whatever it has to be."
Source: http://www.chicagotribune.com/technology/chi−0610150241oct15,1,1992288.story?track=rss

10. *October 14, Associated Press* — **Government reports 788 cases of lost data.** Federal workers at 19 agencies have lost personal information affecting thousands of employees and the public, raising fresh concerns about the government's ability to protect sensitive information. Most of the data was lost or stolen. In a few cases, it was accessed by computer hackers, according a report released Friday, October 13, by the House Government Reform Committee. In all, the committee reported 788 incidents involving the loss or compromise of sensitive personal information since January 1, 2003. That was in addition to the "hundreds of security and privacy incidents" at the Department of Veterans Affairs, the report said. "Data loss is a government−wide occurrence," the report said. "The vast majority of data losses arose from physical thefts of portable computers, drives and disks or unauthorized use of data by employees." The committee asked all Cabinet agencies, the Office of Personnel Management and the Social Security Administration to report all losses of sensitive personal information since January 2003. In many of the newly reported cases, the agencies still don't know the extent of the losses, the report said.
Report: http://reform.house.gov/UploadedFiles/Agency%20Breach%20Summary%20Final%20(3).pdf
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/13/AR2006101301390.html

11. *October 14, Register (UK)* — **MySpace phishing scam targets music fans.** Con−men have developed a phishing attack targeting MySpace music fans that highlights the evolving use of social engineering techniques in money−making spam e−mails. Junk e−mails featuring the attack have been spammed out to thousands of computer users around the globe in the last week, to trick them into visiting one of a series of bogus Websites that pose as an online music store. The e−mails typically pose as MySpace contact e−mails, increasing the chances that prospective marks will be duped by the messages. The goal of the attack is to trick prospective marks into handing over their names and credit card information to scammers. MySpace boasts an estimated 43 million users, far more than any online bank, so even though their spam e−mails are being distributed indiscriminatingly they are far more likely to reach users of the targeted service, as Fortinet notes. Fortinet has recorded more than 50,000 of these spam emails over the past nine days. The attack, which originally targeted surfers in Japan, has spread worldwide and uses a variety of bogus Websites.
Source: http://www.channelregister.co.uk/2006/10/14/myspace_phishing__scam/

12. *October 14, Reuters* — **Online brokerage account scams worry SEC.** High−tech crooks are hijacking online brokerage accounts by using spyware and operating from remote locations, sometimes in Eastern Europe, U.S. market regulators said on Friday, October 13. The computer "incursions" are a growing problem, said Walter Ricciardi of the U.S. Securities and Exchange Commission (SEC). About 25 percent of U.S. retail stock trades are made by online investors

through roughly 10 million online accounts, according to brokerages regulator NASD. Crooks will load a victim's computer or a public PC with a spy program to monitor a user's activities and capture vital information, such as account numbers and passwords. The program then e−mails the stolen information back to the thief, who can use it to open the victim's accounts. Once inside, the thief may sell off an account's portfolio and take the proceeds. Or electronically hijacked accounts may be used for "pump−and−dump" schemes to manipulate stock prices for profit, Ricciardi said. Public computers in such places as Internet cafes and hotel rooms are especially vulnerable to incursions. But home computers may also be hit as spyware can be imported simply by opening an e−mail attachment.
Source: http://news.com.com/Online+brokerage+account+scams+worry+SEC/2100−1029_3−6125991.html?tag=cd.lede

13. *October 13, Websense Security Labs* — **Multiple Phishing Alert: BB&T Branch Banking & Trust, Teachers Credit Union.** Websense Security Labs has received several reports of phishing attacks that target bank customers. Each of the phishing e−mails below provide a link to a phishing site that attempts to collect user account information.
BB&T Branch Banking & Trust: Users receive a spoofed e−mail message, which claims that after a review their account has been suspended until they update it. Users are asked to log on to make these updates.
Teachers Credit Union: Users receive a spoofed e−mail message, which claims that if they take part in a survey, they will get $50 credited to their account. Users are asked to log on to verify these changes.
Screenshots:
http://www.websensesecuritylabs.com/alerts/alert.php?Ale rtID=663
http://www.websensesecuritylabs.com/alerts/alert.php?Ale rtID=662
Source: http://www.websensesecuritylabs.com/

[Return to top]

Transportation and Border Security Sector

14. *October 16, News−Review (OR)* — **Train derailment stalls Oregon particleboard plant.** Work halted at a Roseburg Forest Products (RFP) particleboard plant Thursday morning, October 12, due to safety reasons after a train derailed and spilled its contents on top of an underground natural gas pipeline. Five cars loaded with two−by−fours derailed at about 8 a.m. PDT Thursday at the south end of RFP's Dillard facility, near a particleboard warehouse. The natural gas pipeline, which supplies energy for RFP's particleboard plant, was shut down as the derailment was cleared from the site. Hefley said cause of the derailment is under investigation, but a broken rail is suspected as a defective part and cause of the crash.
Source: http://www.newsreview.info/article/20061013/NEWS/61013049

15. *October 16, Chicago Tribune* — **Skycaps expand their service.** There's a new option for travelers at Chicago's O'Hare International Airport. For an extra fee, passengers who drive to the airport and park in the economy lots can check in baggage and receive their airline seat assignments and boarding passes at a staffed kiosk in Parking Lot E. Passengers then can board the free airport transit system, or People Mover, in Lot E, ride to the terminals and go directly to security checkpoints and aircraft gates, the Chicago Department of Aviation said. O'Hare

officials hope the remote skycap service will get passengers on their way quicker and help reduce long lines that form at airline ticket counters. The remote skycap service, which charges $5 per bag, is available on domestic flights only that are operated by American Airlines, United Airlines, Continental Airlines, Delta Airlines, and Alaska Airlines. Many airlines charge for curbside skycap service. Trucks transport baggage in locked compartments from Lot E to the airline terminals, where the bags are screened under the normal protocol by the security agency, officials said. Employees of the baggage service have undergone FBI background checks.
Source: http://www.chicagotribune.com/travel/chi−0610160002oct16,0,1788631.column?coll=chi−homepagetravel−hed

16. *October 16, Customs Help* — **CBP reports ACE now deployed at all land border ports in New York.** U.S. Customs and Border Protection (CBP) has announced that it has completed installations of the Automated Commercial Environment (ACE) at all land border ports in New York. ACE is now available at the ports of Champlain, Cannon Corners, Mooers, Overton Corners, Rouses Point, Trout River, Chateaugay, Fort Covington, Churubusco, Jamieson Line, Massena, Ogdensburg, Alexandria Bay, and Buffalo, which includes the Peace Bridge and the Lewiston Bridge. ACE is the commercial trade processing system being developed by CBP to enhance border security and expedite legitimate trade. The system provides CBP with the ability to collect electronic manifests for trucks. It also provides the trade community with additional capabilities to comply with Trade Act of 2002 requirements for the electronic transmission of advance manifest information to CBP.
Source: http://www.customshelp.com/customshelpweb/index/news−and−events/customs−news.htm?articleId=335

17. *October 16, 1010 WINS (NY)* — **Subway turnstile could detect explosives.** A company that designs bomb−sniffing scanners used by the New York Metropolitan Transit Authority is creating a prototype subway turnstile that would spot passengers carrying explosives. Mark Elliott, a vice president of Smith Detection, says the turnstiles could block a bomb−toting passenger from entering the system.
Source: http://1010wins.com/pages/108769.php?contentType=4&contentId =223725

[Return to top]

Postal and Shipping Sector

18. *October 16, KHAS−TV (NE)* — **Nebraska emergency officials simulate post office disaster situation.** Emergency officials in Hall County, NE, teamed up Saturday, October 14, for a "weapons of mass destruction" disaster drill. Everything seemed quiet at the Grand Island processing distribution facility for the United State post office before sunrise, but within moments, things changed and the full−scale emergency exercise was underway. And that planning paid off as over 30 people from 10 different agencies participated in the decontamination process of a simulated anthrax release. The Hall county emergency management director agrees all of the different agencies worked very well together through out the entire drill.
Source: http://khastv.com/modules/news/article.php?storyid=6920

19. *October 15, News & Observer (NC)* — **Postal Service adding branches in stores.** The U.S. Postal Service is trying to be more convenient and competitive. First it opened automated postal centers in some post office lobbies, and now it has licensed postal outlets inside retail stores. Currently, North Carolina has 45 contract postal units, including three in the Triangle. The post office is considering another in the Brier Creek area in Raleigh. They are like miniature post offices, with official post office signs, packaging and an official blue mail−drop slot. A post office representative picks up the mail daily Monday through Saturday, and there are extended Saturday hours. What you can do there: Most of what you can do at a regular post office, except money orders, passports, post office boxes, and overnight international mail. The post office provides money selling items and postage to the shop owner, who sells them to the customers. The post office pays the owner a small percentage of the sales.
Source: http://www.newsobserver.com/104/story/498889.html

[Return to top]

Agriculture Sector

20. *October 15, Associated Press* — **Winter spinach demand worries farmers.** Spinach grower Jack Vessey may struggle to break even this year if consumers remain wary about eating spinach after an E. coli outbreak killed three people and sickened nearly 200 others nationwide. The contamination was traced to the Salinas Valley, CA −− more than 400 miles to the north of Vessey's fields. Even so, it threatens his bottom line as uncertain demand wreaks havoc with his growing schedule. Spinach is big business in the Imperial Valley of California and Yuma, AZ. The areas along the U.S.−Mexico border account for nearly all the winter spinach grown in this country. Imperial Valley produced more than 30.5 million pounds of the vegetable in 2005 with a gross value of $19.8 million. Lagging consumer confidence has left farmers wondering how much to plant during the season that runs from October to February. "Farmers had to take a long look at planting at all," added Aryon Schoneman, executive director of the Imperial Valley Vegetable Growers Association. Vessey & Co. Inc., the largest of about 10 growers in the valley, has cut spinach production in half from this time last year.
Source: http://www.breitbart.com/news/2006/10/15/D8KP6ANO0.html

[Return to top]

Food Sector

21. *October 15, Canadian Press* — **Researchers find C. difficile in variety of meat products in U.S., Canada.** C. difficile bacteria have been found in a variety of ground and processed meats bought from grocery stores in Canada and the U.S., an unexpected discovery some experts say may be linked to recent baffling changes in the pattern of the disease. Some of the U.S. meats contained the hypervirulent C. difficile strain responsible for severe outbreaks in hospitals in Quebec, Canada, and parts of the U.S. over the past few years. Two teams of researchers, at the University of Arizona and at the Ontario Veterinary College, found C. difficile spores in some samples of ground beef, veal, turkey and pork, pork sausage, chorizo, summer sausage and liverwurst. Nearly 30 percent of the meats tested in Arizona and 18 percent tested in Ontario contained C. difficile. Each team bought meat over a period of several months from three

different grocery stores in Tucson, AZ, and in the Guelph, Ontario. The two projects were conducted independently.
C. difficile information: http://www.cdc.gov/ncidod/dhqp/id_Cdiff.html
Source: http://www.breitbart.com/news/na/cp_x101511A.xml.html

22. *October 14, Associated Press* — **Test of food warnings failed often.** A warning system meant to alert food companies in the event of a food poisoning outbreak failed one−third of the time in a recent government test. The U.S. Food and Drug Administration (FDA) was able to reach an emergency contact for a food facility in two out of every three cases. Developed in response to the September 11 attacks, the system is supposed to help the government track the source of an outbreak of foodborne illness and help notify companies that might be affected. In the test, conducted from July 10 to August 2, the agency got responses from or talked with emergency contacts who were registered by facilities about 66 percent of the time. The rate was 72 percent for U.S. facilities and 59 percent for foreign facilities. But FDA reached the right emergency contact only 55 percent of the time. People told the FDA that they were not emergency contacts at 10 percent of U.S. facilities and 11 percent of foreign facilities.
FDA report: http://www.cfsan.fda.gov/~furls/ffregacc.html
Source: http://www.rrstar.com/apps/pbcs.dll/article?AID=/20061014/BU SINESS/110140046

[Return to top]

Water Sector

23. *October 12, U.S. Environmental Protection Agency* — **New rule for the protection of underground drinking water.** More than 100 million Americans will enjoy greater protection of their drinking water under a new rule issued Thursday, October 12, by the U.S. Environmental Protection Agency. The rule targets utilities that provide water from underground sources and requires greater vigilance for potential contamination by disease−causing microorganisms. The risk−targeting strategy incorporated in the rule provides for: regular sanitary surveys of public water systems to look for significant deficiencies in key operational areas, triggered source−water monitoring when a system that does not sufficiently disinfect drinking water identifies a positive sample during its regular monitoring to comply with existing rules, implementation of corrective actions by ground water systems with a significant deficiency or evidence of source water fecal contamination, and compliance monitoring for systems that are sufficiently treating drinking water to ensure effective removal of pathogens.
Source: http://yosemite.epa.gov/opa/admpress.nsf/74de46851771ad92852 5702100565d7d/026a2a41917cfa678525720500568809!OpenDocument

[Return to top]

Public Health Sector

24. *October 16, Associated Press* — **Doctors need more bioterror training.** Asked to tell which of five likely bioterror weapons would cause specific symptoms, emergency room doctors in Chicago, IL, did poorly. The 36 physicians and 37 doctors in training missed more than

two−thirds of the questions about chemical weapons and more than half of those about biological agents, according to a report presented Sunday, October 15, at the convention of the American College of Emergency Medicine in New Orleans, LA. The study is disturbing but too small to make any conclusions about emergency room doctors in general, said Peter DeBlieux. A much larger study of residents −− doctors in training −− in the more general field of internal medicine found last year that they misdiagnosed diseases that could be spread as weapons of terror more than half the time. It also found that they did quite well after Internet−based training.
Source: http://www.suburbanchicagonews.com/heraldnews/news/98427,4_1_JO16_DOCTORS_S1.article

25. *October 16, Agence France−Presse* — **Indonesia's bird flu toll jumps to 54.** Indonesian health authorities have confirmed another person has died of bird flu, bringing the national toll from the H5N1 virus to 54 −− the highest in the world. Samples taken from a 67−year−old woman who died Sunday, October 15, returned positive results from two laboratories, the health ministry said.
Source: http://news.yahoo.com/s/afp/20061016/hl_afp/healthfluindones ia_061016043847

[Return to top]

Government Sector

26. *October 16, Forbes* — **Man allegedly climbs White House fence.** The Secret Service on Saturday, October 14, apprehended a man who climbed over the fence along the north lawn of the White House. Around 6:30 p.m. EDT, Alexis Janicki, 24, jumped the fence, said Secret Service spokesperson Kim Bruce. He was immediately apprehended by the Secret Service uniformed division and taken into custody. Janicki was charged with trespassing and possession of a controlled substance, which was cannabis, Bruce said. He was turned over to the District of Columbia's Metropolitan Police Department for processing.
Source: http://www.forbes.com/business/energy/feeds/ap/2006/10/14/ap_3091386.html

27. *October 14, KSL News (UT)* — **Fire forces evacuation of Utah county jail.** Inmates at the Summit County Jail were temporarily evacuated Saturday, October 14, when guards smelled smoke between two rooms. The inmates were moved from the jail to a safe hallway. They never left the building. Firefighters say the smoke was caused by smoldering lint that may have come from heaters on the roof. Guards say the evacuation was done according to plan.
Source: http://www.ksl.com/?nid=148&sid=566733

[Return to top]

Emergency Services Sector

28. *October 16, Advocate (LA)* — **New rule in Louisiana gives first responders additional post−hurricane information.** A new Louisiana emergency rule hopes to give first responders more information about possible post−hurricane hazardous waste. Under the new emergency rule, industries or companies in control of rail cars, barges and other temporary or mobile

vehicles that contain hazardous material must report information to a state hotline within 12 hours of a parish−declared mandatory evacuation. The emergency rule will be in effect for the next several months until a final rule can be written and put to a public hearing in January. The rule only applies to a Category 3 or stronger hurricanes and does not include material contained in trucks. Facilities also do not have to report material unless is it is in larger amounts or it is different from what they annually report to state and federal authorities.
Source: http://www.2theadvocate.com/news/4406716.html

29. *October 16, Public Opinion (PA)* — **Regional drill tests response to major terror attack in Pennsylvania.** Saturday, October 14, an eight−county regional disaster drill was conducted to test the effectiveness of south central Pennsylvania's response to a major terrorist attack. The exercise not only put deficiencies such as different radio frequencies to the test but also tested the different counties' ability to communicate with each other. Three national firms will evaluate the exercise and issue a report in a few weeks. Each part of the exercise −− in Franklin, York and Lancaster counties −− addressed more than 50 federal guidelines for response to terrorist attacks. The official report by the evaluators will show how well those guidelines were addressed and where shortcomings might lie. Meanwhile, Duane Hagelgans, public information officer at the task force's communications center in Lancaster, said the exercise seemed to be a success. "We were able to coordinate with all the counties without problems," he said.
Source: http://www.publicopiniononline.com/localnews/ci_4498793

[Return to top]

Information Technology and Telecommunications Sector

30. *October 13, Secunia* — **Microsoft PowerPoint unspecified code execution vulnerability.** A vulnerability has been reported in Microsoft PowerPoint, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified error when processing PowerPoint presentations. According to Microsoft, the vulnerability may allow execution of arbitrary code. The vulnerability is reported in Microsoft PowerPoint 2003. Other versions may also be affected.
Solution: Do not open untrusted Office documents.
For more information, see: http://www.techweb.com/wire/security/193301873;jsessionid=3YXNKK1BIDQACQSNDLRSKH0CJUNN2JVN
Source: http://secunia.com/advisories/22394/

31. *October 13, CNET News* — **Security firms skeptical about Vista shift.** On Friday, October 13, Microsoft said it will give security software makers technology to access the kernel of 64−bit versions of Vista for security−monitoring purposes. Additionally, the company said it will make it possible for security companies to disable certain parts of the Windows Security Center in Vista when a third−party security console is installed. Microsoft made both changes in response to antitrust concerns from the European Commission. Led by Symantec, the world's largest antivirus software maker, security companies had publicly criticized Microsoft over both Vista features and also talked to European competition officials about their gripes. Security companies are taking note of the changes Microsoft said it would make to the operating system update, but will judge the outcome when they actually see them. "We have

not seen anything yet," said Cris Paden, a Symantec spokesperson. "These are technical issues. Until we actually see the [application program interfaces], all we know is what they have said in the media. So far they have not done anything yet."
Source: http://news.com.com/Security+firms+skeptical+about+Vista+shift/2100−7355_3−6125866.html?tag=nefd.top

32. *October 13, IDG News Service* — **Windows CE, Symbian wide open to attack.** Windows CE is at an especially high risk of attack according to a new analysis of malware threats. Kaspersky Lab researcher Alexander Gostev has produced the report, it which it is noted that the mobile version of Windows remains wide open to software exploits compared to desktop versions, and allows easy programming access to core operating system functions. Gostev refers to the growing number of vulnerabilities that have affected the platform. "The main environment used to develop malicious programs will be .Net, and a significant number of these viruses will exploit vulnerabilities in Windows CE," said Gotsev. Although rival Symbian is a harder platform on which to create native malware, Gotsev is almost as scathing on its security design. He details a newly documented and verified vulnerability that would allow an attacker to cause a denial−of−service on a Symbian system simply by sending a small file capable of choking the Web browser, thereby slowing it down.
Part 1 of Gosev's report: http://www.viruslist.com/en/analysis?pubid=200119916
Part 2: http://www.viruslist.com/en/analysis?pubid=201225789
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004131&source=rss_topic85

33. *October 13, VNUNet* — **Companies urged to check IE7 readiness.** Microsoft's upgrade to Internet Explorer (IE) will be automatically pushed to desktops later this month, but a Web testing firm has warned that many companies may not be ready. According to the IE Blog, Internet Explorer 7 will be released this month and pushed out to customers via Automatic Updates a few weeks later. Deri Jones, chief executive at Web testers SciVisum, claimed that, although IE7 appears to be more standards−compliant than the previous release, it still contains many bugs. As Microsoft has decided to push the upgrade through Windows Update within weeks of IE7's release, many users are going to be upgraded without really being aware.
Source: http://www.vnunet.com/vnunet/news/2166348/ie7−coming−firms−r eady

34. *October 12, Security Focus* — **Spying on bot nets becoming harder.** The workings of bot nets will become more difficult to divine in the future, because the people who control the networks are moving away from using Internet Relay Chat rooms to link the compromised computers together, a security researcher told attendees at the Virus Bulletin 2006 conference. José Nazario, a senior security researcher for Arbor Networks, spent more than six months delving into the chat rooms typically used by bot herders as the central command posts for their compromised networks. The research, which was part of a project dubbed "Bladerunner," used a mock bot that Nazario and an intern at Arbor coded using Python. The researchers found that the command and control channels are increasingly becoming encrypted and are increasing moving away from chat rooms to Web servers.
Source: http://www.securityfocus.com/brief/328

35. *September 01, Department of Homeland Security* — **DHS OIG releases report on its information security program.** The Department of Homeland Security (DHS) Office of

Inspector General (OIG) has released a report entitled, "Evaluation of DHS' Information Security Program for Fiscal Year 2006." This report assesses the strengths and weaknesses with employees and officials of DHS, direct observations, and a review of applicable documents.
Source: http://www.dhs.gov/interweb/assetlibrary/OIG_06−62_Sep06.pdf

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4662 (eDonkey2000), 113 (auth), 80 (www), 139 (netbios−ssn), 445 (microsoft−ds), 6082 (−−−), 25 (smtp), 135 (epmap), 6346 (gnutella−svc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

36. *October 16, Associated Press* — **Hawaii on edge after 6.7−magnitude quake.** Officials began inspecting bridges and roads across Hawaii early Monday, October 16, following the strongest earthquake −− that hit at 7:07 a.m. local time on Sunday, 10 miles north−northwest of Kailua−Kona, on the west coast of Hawaii Island, known as the Big Island −− to rattle the islands in more than two decades. At least one stretch of road leading to a bridge near the earthquake's epicenter on the Big Island collapsed, Civil Defense Agency spokesperson Dave Curtis said Monday. Several other roads on the Big Island were closed by mudslides, debris, and boulders, but most were still passable, he said. The power outages were largely due to power plants turning off automatically when built−in seismic monitors were triggered by the quake. About a dozen schools were closed for inspection, but no major injuries or deaths have been reported. A government computer simulation estimated as many as 170 bridges could have been damaged by the quake, said Bob Fenton, Federal Emergency Management Agency director of response for the region. The shaking broke water pipes at ResortQuest Kona By The Sea, turning the front of the building into a dramatic waterfall starting at the fourth floor, said Kenneth Piper, who runs the front desk.
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20061016/NEW S99/61016006

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.